Week 4- Implementing Cloud Logging and Monitoring

Name- Samruddhi Dattu Nikam

PRN- 2124UCSF2019

College Name- Sanjivani University

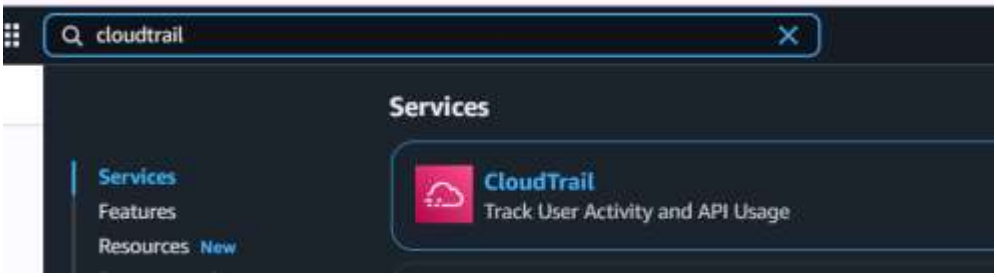
Email Id- samruddhi.nikam_24ucs@sanjivani.edu.in

❖ **Task-** 1) Enable CloudTrail/Cloud Audit Logs.
2) Configure alerts for suspicious activity.
3) Document findings.

Step Enable Cloud Trail/ Cloud Audit Logs.

Step 1: Login to AWS Console

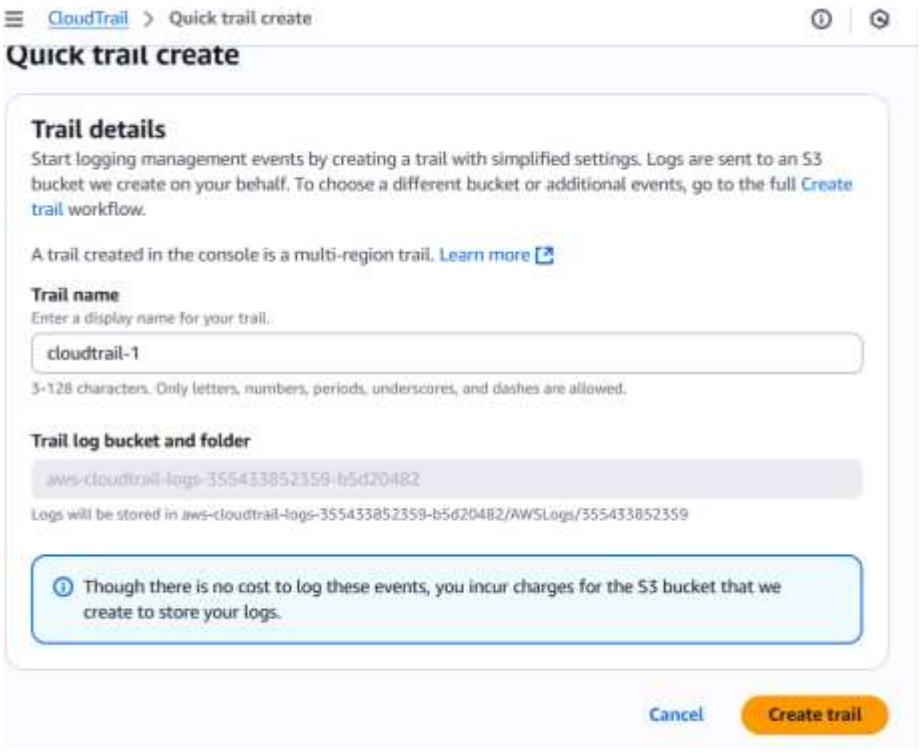
Step 2: Search and open CloudTrail from the Services menu.

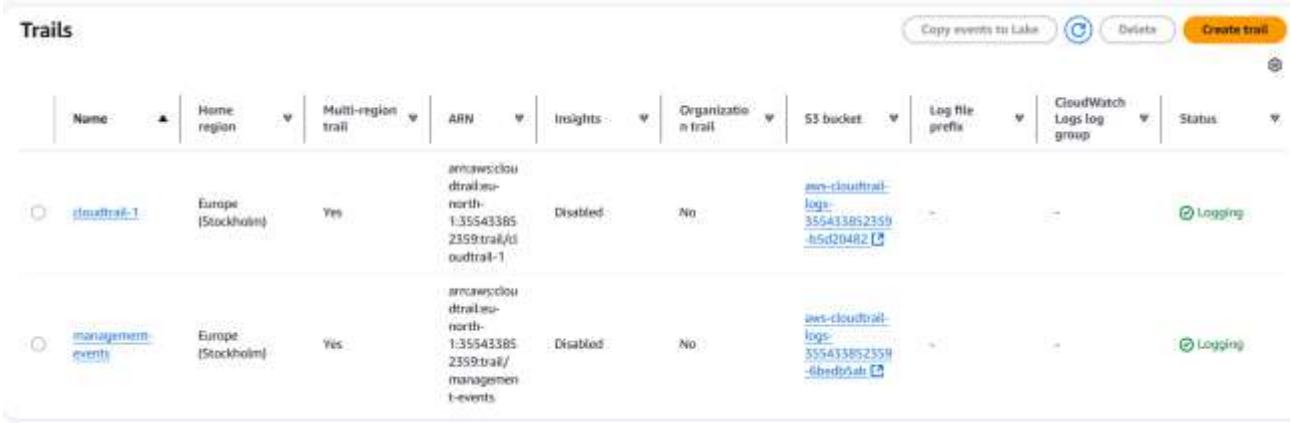


Step 3: Click Create trail.

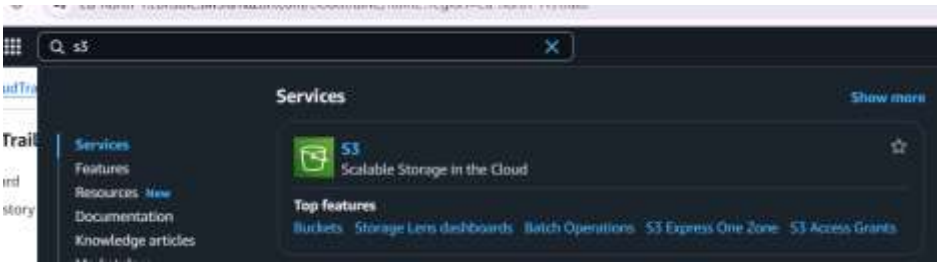
Week 4- Implementing Cloud Logging and Monitoring

Step 4- Fill in trail Name cloudtrail-1, and then click create trail.





Step 5- Set up S3 Bucket to store logs: create new bucket.

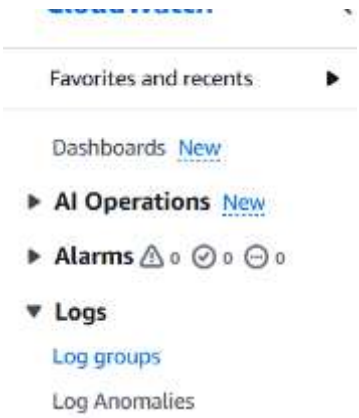


Week 4- Implementing Cloud Logging and Monitoring

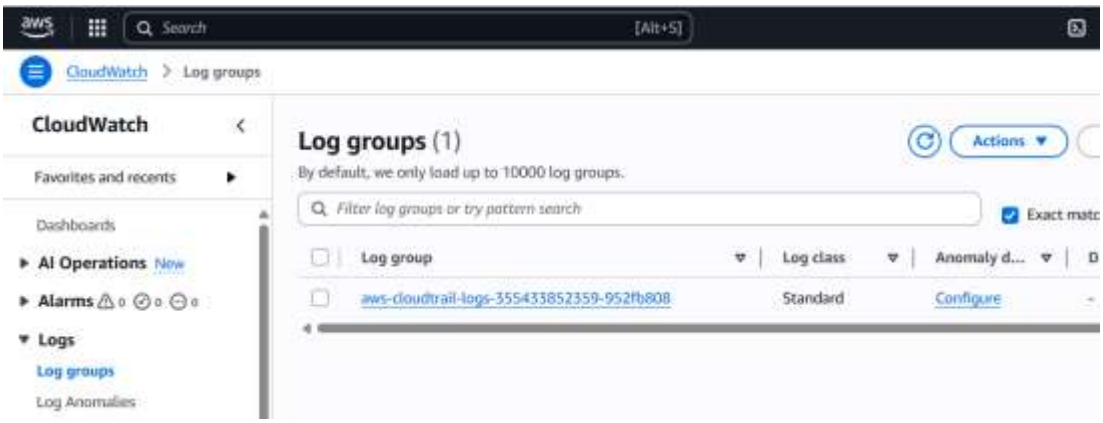
Step 6- Enable CloudWatch Logs, Create new Log Group: /aws/cloudtrail/logs, Allow to create IAM role automatically, then Click Create trail.

Task 2- Configure alerts for suspicious activity.

Step 1-Go to CloudWatch , Log Groups

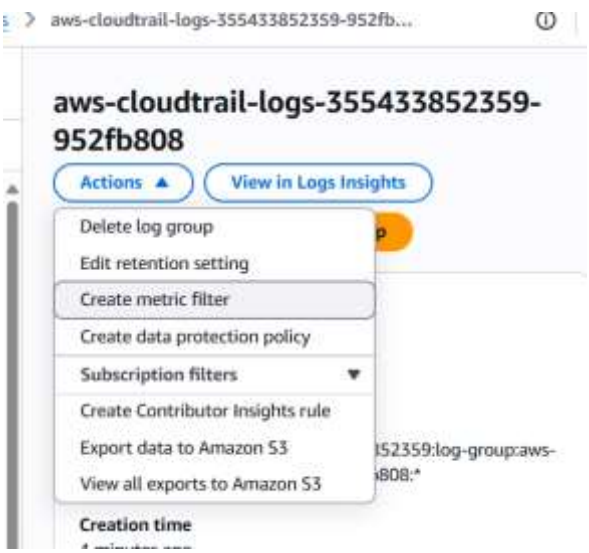


Step 2- Select your log group: /aws/cloudtrail/logs

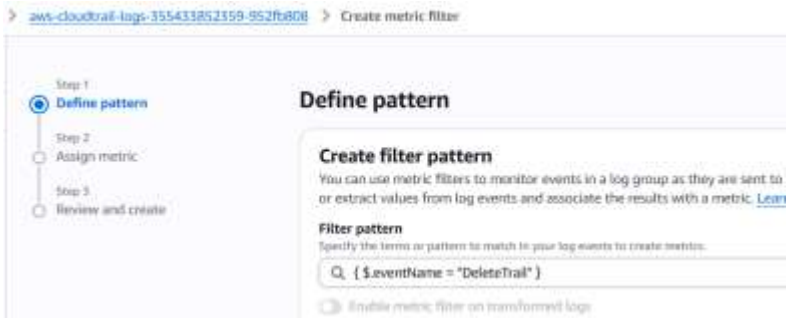


Step 3- Click Actions → Create Metric Filter

Week 4- Implementing Cloud Logging and Monitoring



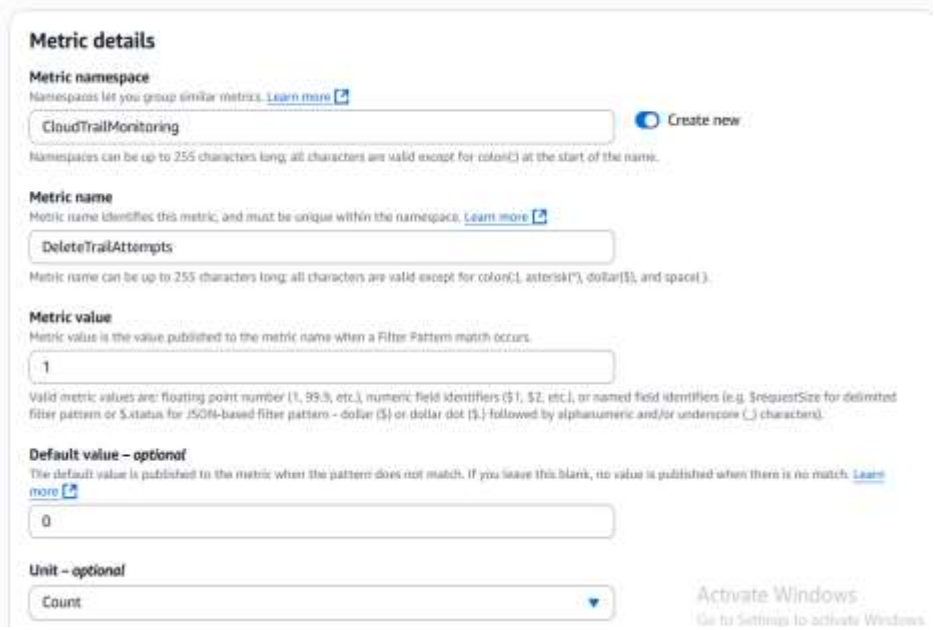
Step 4- Paste filter pattern, and then click next.



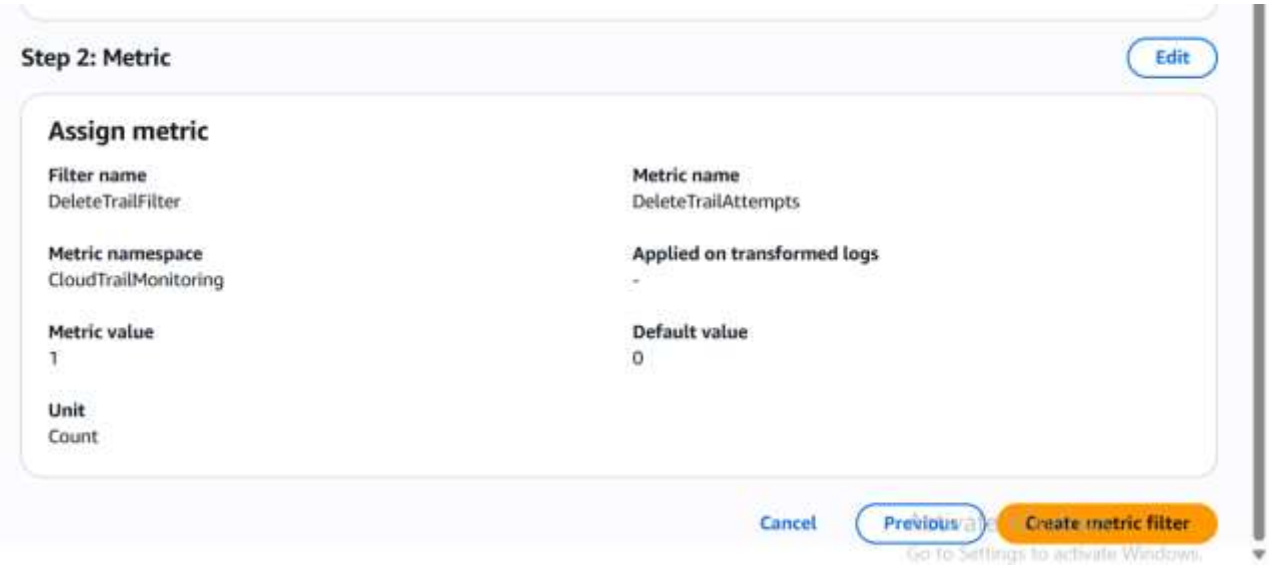
Step 5- next step is create filter name, enter the filter name.

Step 6- Then Enter the Matrix Details.

Week 4- Implementing Cloud Logging and Monitoring



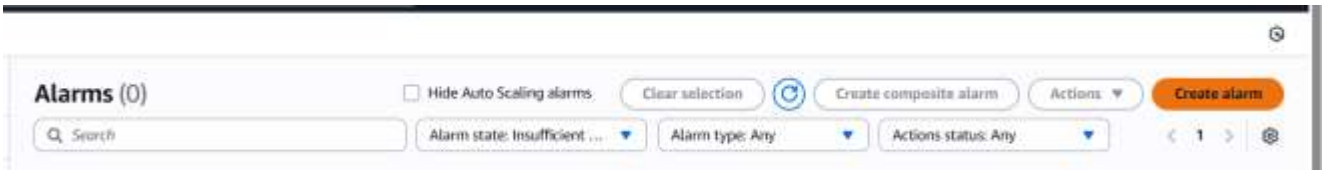
Step 7- Then click Create Matrix.



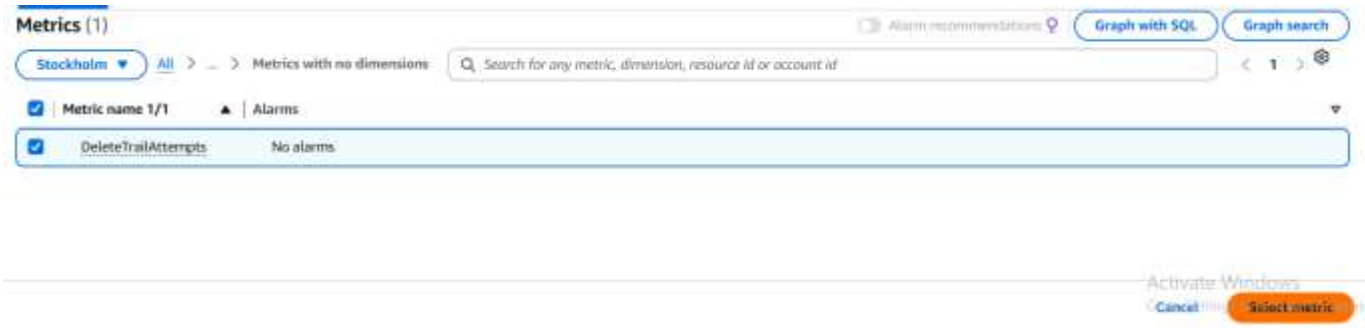
Step 8- Matrix filter Created successfully.

Week 4- Implementing Cloud Logging and Monitoring

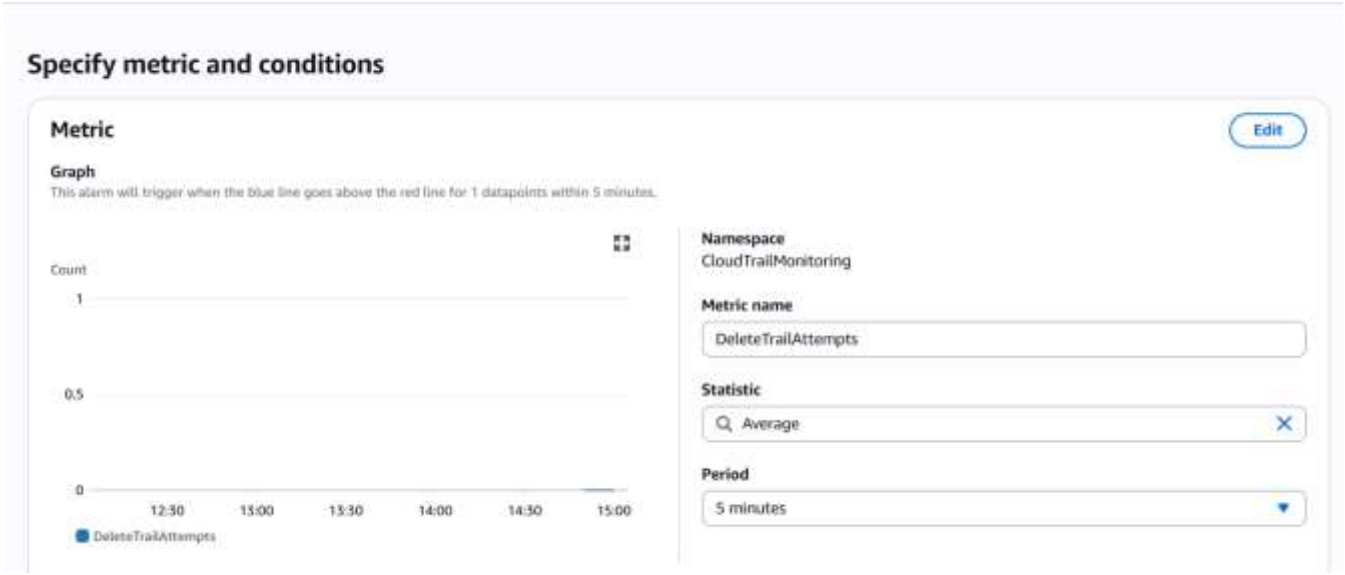
Step 9- Go to CloudWatch → Alarms → Create Alarm



Step 10- Select metric.

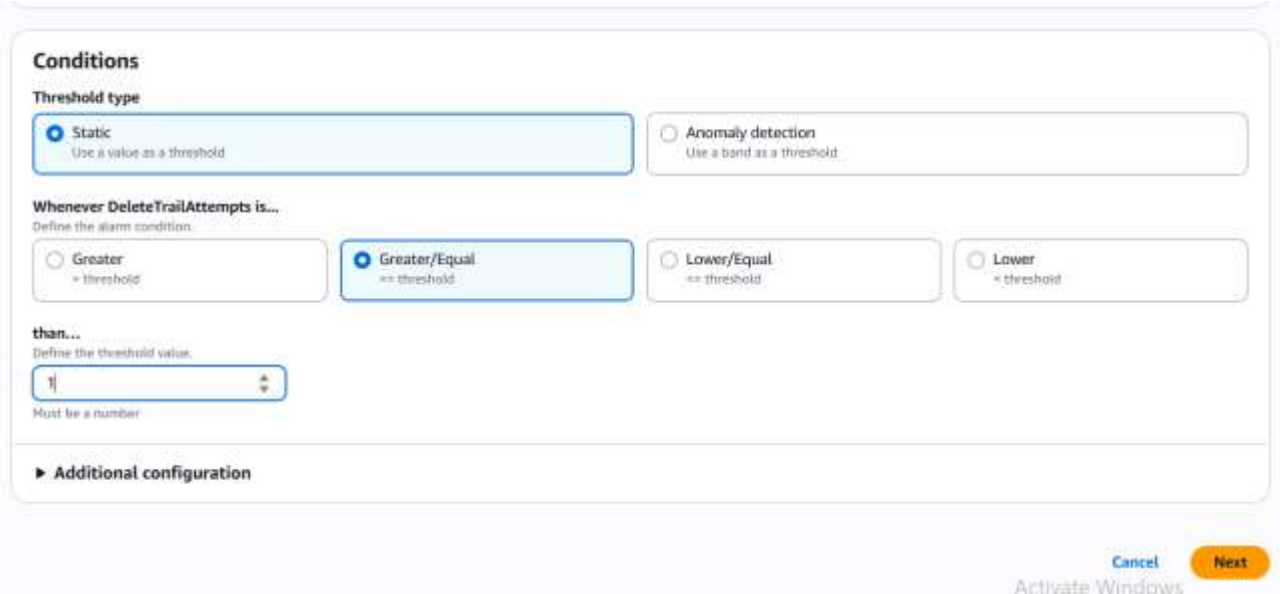


Step 11- Set threshold: Static, Condition: Greater than or equal to 1, Period: 5 minute.

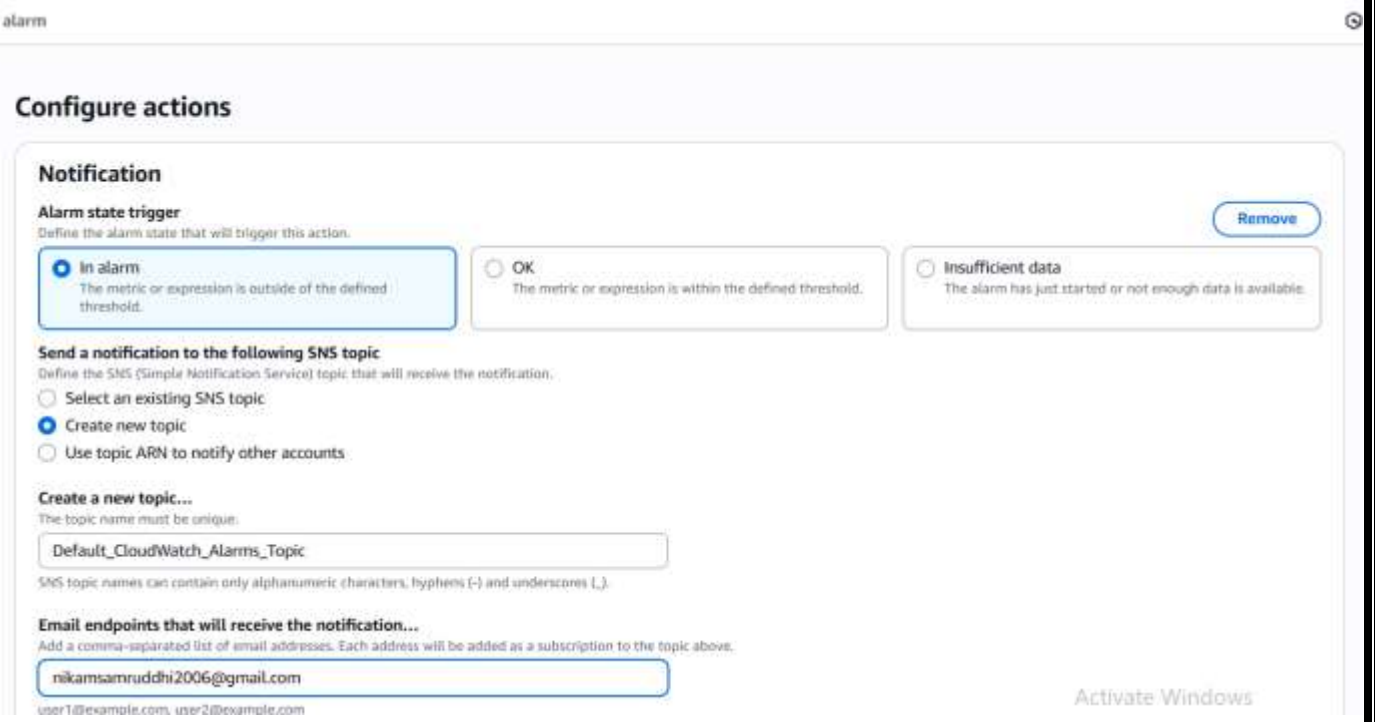


Week 4- Implementing Cloud Logging and Monitoring

Step 12- Set Condition, and then click Next.

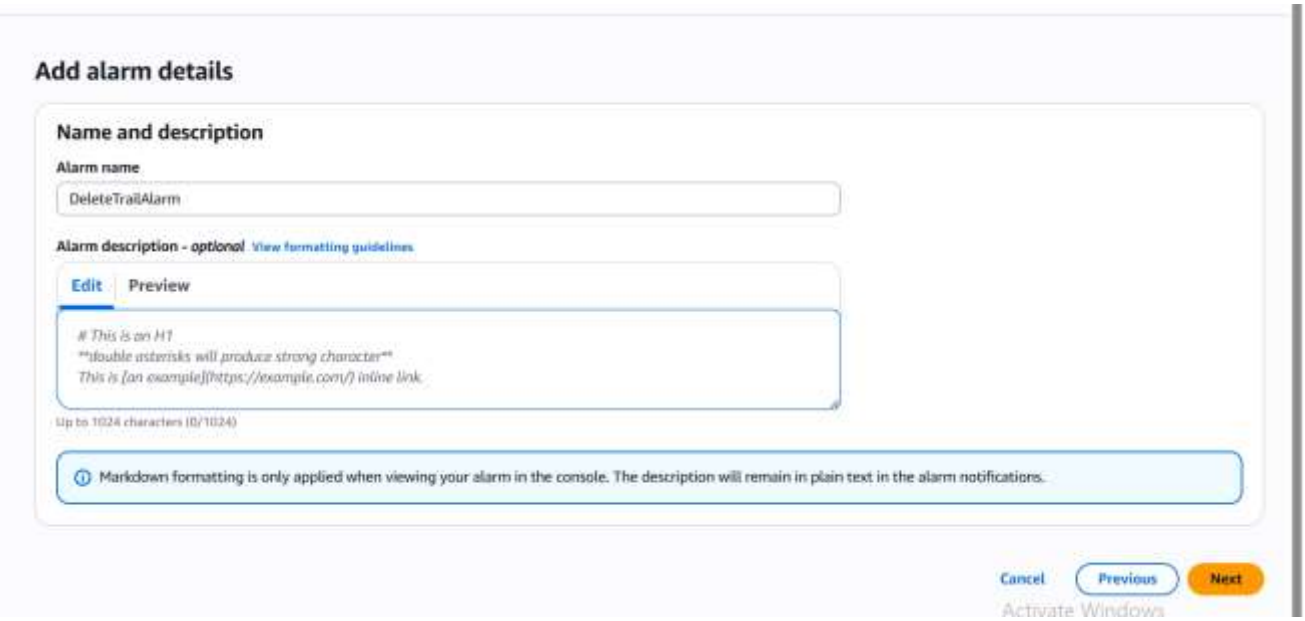


Step 13- Add Configure Action Details.



Week 4- Implementing Cloud Logging and Monitoring

Step 14- Add Alarm Details, and then click next.



Step 15- Set Alarm Successfully.